

2/ppts

10/538420

1

JC17 Rec'd PCT/PTO 08 JUN 2005

**TRANSFER OF PACKET DATA IN SYSTEM COMPRISING MOBILE TERMINAL,  
WIRELESS LOCAL NETWORK AND MOBILE NETWORK**

**BACKGROUND OF THE INVENTION**

**[0001]** The invention relates to the transfer of packet-switched data in a system comprising a mobile terminal, a wireless local network and a mobile network.

**[0002]** Packet-switched data transmission services have been developed for mobile terminals. GPRS services (General Packet Radio Service) are widely used in terminals supporting the GSM radio technology and packet-switched services of the 3GPP system (Third-Generation Partnership Project) based on the WCDMA (Wideband Code Division Multiple Access) radio technology are also based on GPRS. PDP contexts are generally logical connections on which IP data are transferred from a mobile station to a boundary node (GGSN) in a GPRS/3GPP network and vice versa. Different PDP contexts may be provided with different quality of service (QoS) properties, thereby enabling optimal transmission of time-critical or error-critical data, for instance. In addition, an IP multimedia subsystem IMS is designed in the 3GPP system for providing various IP multimedia services to 3GPP mobile stations (UE; User Equipment). The IMS utilizes PDP contexts for data transfer to or from a mobile station. The IMS includes functions that enable the negotiation of an end-to-end session on the application plane using the SIP protocol (Session Initiation Protocol), the features of the session being for instance the codecs used, the termination points and the quality of service (QoS). For arranging the negotiated end-to-end quality of service also in the 3GPP network, a service based local policy (SBLP) is applied. The IMS includes a call session control function (CSCF), which includes a PDF function (Policy Decision Function) for authorizing quality of service resources (bandwidth, delay, etc.) for an IMS session based on SIP-layer SDP information (Session Description Protocol).

**[0003]** Besides access via the conventional access networks of the PLMN (Public Land Mobile Network) networks, such as the BSS (Base Station Sub-system) of the GSM, a need has also risen to allow access to the services of a PLMN by local networks primarily targeted at providing high speed data transmission in a limited area, such as in an office building. WLAN (Wireless

Local Area Network) technologies are very popular today and standardization work has been done in 3GPP to define WLAN-3GPP interworking. This interworking may include the usage of 3GPP subscriber management procedures, such as authentication and charging procedures, as well as data transmission via the 3GPP core network for mobile terminals in a WLAN network. The basic concept is to provide a 3GPP subscriber with access via a WLAN network, also when roaming abroad. 3GPP specification TS 23.234 "3GPP system to Wireless Local Area Network (WLAN) interworking", version 6.0.0, March 2004, defines the system description for WLAN-3GPP interworking.

[0004] For WLAN interworking, the 3GPP network is provided with some new network elements or entities. A WLAN Access Gateway (WAG) is a gateway via which the data to/from the WLAN Access Network is transferred to provide the MS with 3G PS based services. A Packet Data Gateway (PDG) is a network element providing access for WLAN roaming mobile terminals to external IP networks, including those supporting 3GPP PS (Packet-switched) domain-based services. An AAA (Authentication, Authorization and Accounting) server may provide authentication and charging services for WLAN roaming mobile terminals.

[0005] It is desirable that end-to-end QoS negotiation also be provided for mobile terminals roaming in WLAN networks. The above-mentioned 3GPP specification TS 23.234 defines on page 29 that the PDG performs the functions of a service-based local policy enforcement point (PEP) and communicates with a policy decision function to allow a service-based local policy. QoS interworking information may be obtained from the policy decision function. IETF RFC (Request For Comments) 2753 "A Framework for Policy-based Admission Control", R. Yavatkar et al., January 2000, describes a framework for providing policy-based control and a client-server protocol for communication between a policy server (PDP; Policy Decision Point) and its client (PEP). However, the 3GPP specification TS 23.234 does not disclose how to arrange the adoption of the policy for the terminal in the WLAN-3GPP interworking system.

## BRIEF DESCRIPTION OF THE INVENTION

[0006] The object of the invention is thus to provide a method and

equipment for implementing the method so as to enable an enhanced data transfer method for terminals visiting a wireless local network. The objects of the invention are achieved by a method, a system, a network element, a wireless terminal, and computer programs, which are characterized by what is stated in the independent claims. Some preferred embodiments are disclosed in the dependent claims.

**[0007]** According to an aspect of the invention, end-to-end service related parameters are signalled via a separate signalling element. A resource authorization identifier is received in the mobile terminal from the signalling element. The resource authorization identifier is transmitted to the mobile network via the local network. Authorization is requested from the signalling element by the mobile network on the basis of the resource authorization identifier. A tunnel between the mobile terminal and the mobile network is bound to the end-to-end data flow of the mobile terminal on the basis of an authorization response received from the signalling element and comprising identification information on the end-to-the end data flow and tunnel identification information identifying the tunnel.

**[0008]** The advantage of the invention is that a policy authorized by a signalling element, such as a SIP end-to-end quality-of-service negotiation signalling element, may be used in a system in which the mobile terminal accesses the mobile network via a wireless local network. Thus, it is possible to arrange a service in the local system comprising the mobile network and the wireless local network on the basis of a confirmation from the signalling element. By the authorization, it is possible to achieve mapping between the data flow in the system of the mobile network and the wireless local network and the end-to-end data flow.

**[0009]** In one embodiment, the authorization may comprise information on the allowed quality of service, and the underlying data transmission resources in the system are adapted according to this QoS information.

#### BRIEF DESCRIPTION OF THE FIGURES

**[0010]** In the following, some preferred embodiments of the invention will be described in detail with reference to the accompanying

drawings, in which

**[0011]** Figure 1 generally illustrates a WLAN-3GPP interworking system;

**[0012]** Figure 2 shows the WLAN-3GPP interworking protocol architecture; and

**[0013]** Figure 3 is a flow diagram of an embodiment of the invention.

#### DETAILED DESCRIPTION OF THE INVENTION

**[0014]** The method of an embodiment is illustrated next with reference to an exemplary WLAN-3GPP interworking system shown in Figure 1. However, the invention is applicable to any packet-switched telecommunication system for mobile terminals visiting wireless local networks. Besides a system incorporating a 3GPP network, the method of the invention is applicable to a system in accordance with a second-generation GPRS service, for instance. The local network is, in accordance with an embodiment, a wireless local area network employing user authentication and network access control according to an IEEE 802.1x standard, such as a wireless local area network according to the IEEE 802.11i standard. However, the invention can also be applied to a system comprising another IEEE 802-based wireless local area network or some other type of local networks, typically to networks operating at un-licensed frequency bands, such as a network according to the BRAN (Broadband Radio Access Networks) standard, a Home RF network or a Bluetooth network. The BRAN standards comprise High Performance Radio Local Area Network HIPERLAN standards of types 1 and 2, HIPERACCESS and HIPERLINK standards.

**[0015]** Reference is made to Figure 1, wherein the main parts of a mobile system include a WLAN access network AN, a 3GPP network part PLMN comprising network elements for WLAN interworking, and a mobile station MS, also called user equipment UE in 3GPP specifications. It is to be noted that the WLAN-3GPP interworking specification work is not finished at the time of filing of the present application, and the basic principles of the present invention can also be applied to modified WLAN-3GPP interworking systems.

**[0016]** The WLAN access network AN and the 3GPP network PLMN can communicate over an IP-based (Internet Protocol) network (IPNW). As shown in Figure 1, the WLAN access network AN can operate as a UMTS access network, and it can also provide access to other networks, such as the public Internet. The WLAN access network AN comprises access elements called access points AP, which provide a mobile station MS with radio access and thus terminate the broadband radio connection. The access point AP controls the L2 radio interface according to the applied radio technology, which means the IEEE 802.11 standard according to one embodiment. The IEEE 802.11 specifications determine both physical-level and MAC-level protocols for data transmission over the radio interface. The data transmission can utilize either infrared or two spread-spectrum techniques (Direct Sequence Spread-Spectrum DSSS, Frequency Hopped Spread-Spectrum FHSS). Both spread-spectrum techniques utilize a 2.4 GHz band. The MAC layer utilizes a CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) technique. The AP also manages the bridging of data streams at the radio interface or the routing thereof to and from other network nodes. It is to be noted that instead of a physical access point, WLAN base station, the term access point AP may also refer to a logical WLAN access point which may be accessed by a number of WLAN base stations. The WLAN access network AN may also comprise further WLAN related network elements, such as a control element or a gateway element GW.

**[0017]** The 3GPP network PLMN may comprise a UMTS terrestrial radio access network UTRAN and a UMTS core network CN, or at least some functionality thereof (not shown in Figure 1). The following describes network elements related to WLAN-3GPP interworking. The 3GPP network PLMN comprises an Authentication, Authorization and Accounting (AAA) server AS, which may provide authentication services and preferably also charging services. Therefore, 3GPP network subscriber data and authentication services can be used for mobile stations MS roaming in the WLAN network AN and comprising a UMTS subscriber identity module USIM and/or a (GSM) SIM. A mobile station MS user does not necessarily have to have a contract made in advance with the WLAN network AN operator. In such a case, an MS can be charged for the wireless connection provided by the WLAN network AN later on via the PLMN. Even though the AAA server AS is shown as a separate element in Figure 1, it can be implemented as part of a PLMN network

element. A HLR/HSS (Home Location Register/ Home Subscriber Server) located within the 3GPP subscriber's home network is the entity containing the authentication and subscription data required for the 3GPP subscriber to access WLAN interworking services. The HLR/HSS includes for example information on the quality of service allowed to a subscriber (user profile) and information for the use of services provided by the IMS. The AS communicates authorization information to WLAN and maintains information on the status of the WLAN mobile stations MS.

**[0018]** If the PLMN is not the home network (HPLMN) of the mobile station MS, i.e. the mobile station MS is roaming in the PLMN, the roamed network must communicate with the HPLMN for purposes of authentication and charging. The HPLMN comprises the HLR/HSS, and typically also an authentication centre AuC calculating authentication vectors. An AAA proxy may relay information between the WLAN and the AAA server AS and carry out subscriber management-related actions in the roamed network. Figure 1 does not show any other HPLMN elements, such as the 3GMSC or the SGSN, via which the connection to the HLR/AuC is typically set up. The 3GPP specifications also refer to the roamed network as a serving network (SN) and to the HPLMN as merely a home network (HN).

**[0019]** A packet Data Gateway PDG is a network element providing access for WLAN roaming mobile stations MS to external IP networks, including those supporting 3GPP PS Domain based services. The packet data gateway PDG operates as a gateway between the packet radio system of the UMTS network and an external packet data network PDN. External data networks include for instance the UMTS or GPRS network of another network operator, the Internet or a private local area network.

**[0020]** The mobile station MS may be a mobile phone, a table computer with a WLAN radio interface adapter, or a PDA device, for instance. There may be mobile stations MS of different classes according to their capabilities. The MS may support data transfer via the WLAN access network AN, UTRAN, and/or some other network such as the BSS of GSM, even substantially simultaneously. The mobile station MS is equipped with an IC card including a (U)SIM utilized by a 3GPP subscriber to access the WLAN network for 3GPP interworking purposes.

**[0021]** The WLAN Access Gateway WAG is a gateway via which the data to/from the WLAN Access Network AN is transferred to provide the MS with 3G PS based services. The WLAN Access Gateway resides in the VPLMN in the roaming case, and in the HPLMN in the non-roaming case. The WAG allows a visited 3GPP network PLMN to generate charging information for users accessing via the WLAN AN in the roaming case, enforces the routing of packets through the PDG, performs collection of per tunnel accounting information, and filters out packets based on unencrypted information in the packets. The WAG will forward packets only if they are part of an existing tunnel or expected messages from the MS (service requests and tunnel establishment messages).

**[0022]** For a more detailed description of various WLAN/3GPP interworking related network elements, reference is made to 3GPP specification TS 23.234, v. 6.0.0, "3GPP to Wireless Local Area Network (WLAN) interworking, System description (Release 6)", March 2004.

**[0023]** A 3GPP packet data system may also comprise many other functions, such as a service control function SCF for intelligent network services, and a charging gateway CGF attending to charging. According to an embodiment, the WLAN-3GPP interworking system supports at least some IMS related features. Figure 1 illustrates a call session control function CSCF, which may have three different roles: Proxy-CSCF (P-CSCF) which comprises a PDF function and transfers SIP messages to other SIP network elements; Interrogating-CSCF (I-CSCF) which is a subscriber home network contact point and determines the serving CSCF (S-CSCF) and forwards SIP requests to the S-CSCF; S-CSCF which is a CSCF controlling the end-to-end session of a mobile station. For a more detailed description of the conventional IMS system features, reference is made to 3GPP specification 3GPP TS 23.228, v.6.5.0 (March 2004), 'IP Multimedia Subsystem (IMS); Stage 2; Release 6'. A suitable method for session establishment and QoS selection in the WLAN-3GPP interworking system utilizing IMS principles is illustrated later in connection with Figure 3.

**[0024]** To obtain the packet-switched services of the WLAN network AN, the mobile station MS has to perform a WLAN technology-specific access procedure, making the location of the MS known at the selected WLAN

network AN. In the case of an IEEE 802.11 network, the MS performs an association procedure. The MS is then able to communicate with an access point AP of the WLAN network. PLMN network selection for the MS may be carried out. Network selection and advertisement procedures are described in Chapter 5.4 of the 3GPP TS 23.234. An authentication procedure may be initiated by the MS by sending a network access identifier (NAI) to the WLAN AP which determines the correct (home) AAA server AS and forwards the authentication request to the correct AAA server AS. The WLAN authentication and authorization by the 3GPP AAA server involves the use of an EAP (Extensible Authentication Protocol) Authentication and Key Agreement (AKA) procedure. The WLAN mobile station MS uses the NAI as identification towards the 3GPP WLAN AAA server AS. In this procedure, the subscriber identity module (SIM) information and corresponding information in HLR may be used. If the authentication is successful, the MS may register as a WLAN user to the 3GPP network PLMN. More details on WLAN access and authorization are described in Chapter 7.2 of the 3GPP TS 23.234 specification.

**[0025]** To receive and transmit packet-switched data, a registered mobile station MS has to activate at least one tunnel. This makes the MS known to the PDG and creates a logical data transfer context at the mobile station MS, the WAG and the PDG. The protocol stack between the MS and the PDG is illustrated in Figure 2. When the tunnel is being established, a remote IP address identifying the mobile station MS, which could be an IPv4 or IPv6 address, is defined for the MS. A local IP address of the MS identifies the WLAN MS in the WLAN AN, i.e. the local IP address is used at the Transport IP layer. The remote IP address can be assigned by the home-PLMN, visited-PLMN or an external IP network. In addition to other tunnel related data, such as the negotiated QoS profile, the remote IP address is defined in tunnel information maintained by the PDG.

**[0026]** The tunnel establishment is not coupled to WLAN access authentication/authorization. The WLAN UE may establish several tunnels in order to access several external IP networks simultaneously. External IP network selection is performed as part of the establishment of each tunnel, and the mobile station MS may indicate a preferred WLAN access point name (W-APN).



**[0027]** According to an embodiment, in order to implement a service-based local policy in the WLAN-3GPP interworking system, the PDG comprises a PEP function (Policy Enforcement Point) similar to that of the 3GPP IMS system. However, there are no PDP contexts and associated mechanisms (as those available for GPRS terminals) for roaming WLAN terminals connecting to the PDG via a WLAN network and the WLAN access gateways. Thus, the policy adoption arrangement in the present WLAN-3GPP interworking system differs from that for GPRS terminals. The PEP function controls the offering of quality-of-service resources to the data flow according to the authorization received from the PDF. For binding the authorization decision, the PDF creates a resource authorization identifier, which may be referred to as an authorization token as in the IMS system, for the session and transmits it to the mobile station MS. When the tunnel is being established, the mobile station MS is configured to send to the PDG an authorization token and at least one flow identifier that constitute binding information. The flow identifier identifies the IP media flow associated with the SIP session. There may be a flow identifier for each media component that is to be transferred end to end. The PDG requests authorization for allocating resources to the session indicated by the binding information from the PDF, which is located at the P-CSCF (Proxy CSCF). The PDF functionality makes a final decision on resource allocation to the session and responds to the PDG.

**[0028]** On the basis of the authorization from the PDF, the PDG arranges binding for the external data flow to a tunnel between the MS and the PDG. The gating/filtering functionality offered by the PEP thus tends to identify a given flow or a group of flows by including information about possible header fields in the form of a set of packet filter parameters, i.e. packet filters. The PEP may be arranged to directly map the data flows received from external networks into the correct tunnels on the basis of the packet filters, one or more packet classification parameters (e.g. destination gate/source IP address) being specified in a packet filter. The packet filter(s) may be completely defined, when establishing the logical application-plane connection for the data flow, from identifying identifiers at the P-CSCF element (PDF function), and transferred to the PDG (PEP function). The PEP function may determine a gate by the packet filters for the data flow which it binds to at least one tunnel based on a tunnel identifier. Packet filters could be tunnel-specific, whereby each packet filter is bound to one tunnel.

**[0029]** Figure 3 shows a signalling diagram illustrating in more detail the establishment or modification of a tunnel between the MS and the PDG when applying a service-based local policy in accordance with a preferred embodiment of the invention. The P-CSCF receives 301 a SIP SDP message including the necessary information about the application-plane session to be set up, such as termination points and the bandwidth requirement. The message 301 may originate for instance from another CSCF element (S-CSCF) because of a session invite request from another party to the application-plane logical connection or the mobile station MS. The PDF function authorizes the quality of service resources (bandwidth, delay, etc.) for the IMS session based on the SDP information. The PDF creates an authorization token for the session and sends 302 the authorization token in an SDP message to the mobile station MS. For a more detailed description of the communication between the P-CSCF (PDF) and the mobile station MS, reference is made to 3GPP specification 3GPP TS 23.207, v. 6.2.0, *'End-to-End QoS Concept and Architecture; Release 6'*.

**[0030]** In one embodiment, the mobile station MS comprises a translation/mapping function adapting 303 the application-plane (or IP-plane) quality of service requirements to the WLAN-3GPP interworking system quality of service parameters, i.e. it specifies the QoS parameters to be requested for the tunnel for user data transmission. When the tunnel is being established, the mobile station MS sends 304 to the selected PDG a tunnel establishment or modification request including not only the conventional data of a tunnel establishment request but also an authorization token and at least one flow identifier, in one embodiment the tunnel identifier. In an alternative embodiment, the mobile station MS does not itself adapt the QoS requirements but the network, preferably the PDG, does the adaptation. In this embodiment, the tunnel establishment message 304 does not specify any MS determined QoS parameters. In a further embodiment, no QoS requirement information is sent from the MS but the PDG determines the QoS on the basis of the authorization from the PDG.

**[0031]** The PDG receives the request 305 and determines the appropriate P-CSCF (PDF) on the basis of the authorization token. The PDG transmits 306 a request to authorize the required resources to the PDF functionality of the P-CSCF indicated by the authorization token. This request

comprises the binding information. When the PDF of the P-CSCF finds the IP flow information corresponding to the request 306, it makes the final decision about allocating resources to the session. The PDF transmits 307 a response including the policy to the PDG. The authorization response includes an authorization token, at least one packet classification parameter (packet classifier) negotiated on the application plane and intended as the filter, and QoS information (maximum QoS). In one embodiment, other information similar to that of the Go interface between the CSCF and the PDG in 3GPP specification 3GPP TS 23.207, v. 6.0.0 *'End-to-End QoS Concept and Architecture (Release 6)'* may also be used.

**[0032]** The PDG typically responds 308 to the decision message 307. If the PDF allows resource allocation, the PDG may then bind the information in the authorization response to an identifier referring directly or indirectly to a tunnel, i.e. to a tunnel already existing or being established between the MS and the PDG. The tunnel between the mobile terminal and the mobile network is thus bound to the end-to-end data flow of the mobile terminal on the basis of the authorization response received 307 from the signalling element and comprising identification information on the end-to-end data flow (for instance the source IP address) and tunnel identification information identifying the tunnel. The PDG can thus arrange a tunnel between the MS and the PDG provided with properties in accordance with the authorization 307 and the request 304. The PDG may check, based on the quality of service information received from the PDF, that the quality of service requested for the tunnel does not exceed the quality of service negotiated on the application plane and authorized by the PDF. In one embodiment, the PDG comprises a translation/mapping function which adapts the authorized QoS information to appropriate QoS parameters in the WLAN-3GPP interworking system. Underlying WLAN and/or 3GPP connection resources may be reserved (309) in accordance with the quality of service adapted by the WLAN-3GPP interworking system, preferably by the PDG, from the quality of service parameters of the IP plane or application plane of the mobile station MS (unless the PDG has had to restrict the requested quality because of subscriber data or its own resource limitations, for example). Based on the response 307, the PDG (PEP function) may in one embodiment generate 309 a logical gate, which implements access control according to the decision of the PDF based on the at least one packet classification parameter obtained

from the PDF as its packet filter parameter for one or more tunnels to the MS. The packet classifier may be based on the IP-address and port number, for instance. The gate is bound 309 to the tunnel being established based on a (tunnel) identifier distinguishing it from other tunnels. Other information received from the PDF may also be stored in the PDG.

**[0033]** In one embodiment, the PDG sends a response 310 to the WAG; however, such response may be not necessary. The PDG may transmit information (possibly via the AAA proxy) for arranging filtering in the WAG according to the policy authorized by the PDF. The WAG may arrange filtering based on this information. The WAG may initiate the establishment of a radio network service, whereby a new WLAN-3GPP bearer is set up or modified 311 for the mobile station MS. If the requested QoS attributes cannot be provided for instance on the basis of the subscription, the WAG informs this to the PDG, which confirms new QoS attributes. The WAG sets the packet flow identifier and the radio priority in accordance with the negotiated QoS and responds 312 to the mobile station MS. In an alternative embodiment, the QoS resources are arranged locally in the WLAN network AN on the basis of the information from the PDG. For instance, the QoS may be arranged locally by WSM (Wi-Fi Scheduled Multimedia) being specified for IEEE 802.11e WLAN technology.

**[0034]** The mobile station MS updates its connection information with the tunnel and the WLAN-3GPP bearer. The MS is now able to send and receive data packets of the logical connection negotiated on the application plane and use the tunnel. After step 312, an application of the mobile station MS or the entity reserving quality of service for it is still able to send the necessary messages to finally activate the end-to-end session. For example, an application using the RSVP protocol may send and receive RSVP path and RSVP response messages, based on which the underlying WLAN-3GPP interworking system transmission resources can also be updated. Besides the above-described features, other features may be performed in the WLAN-3GPP interworking system during tunnel establishment/modification. As an example, the PDG contacts the AAA server AS for authorization of the MS.

**[0035]** The PDG is then able to transfer received downlink packets fulfilling the filter conditions defined for the gate to the mobile station using the tunnel that is associated with the gate. When a packet is received 313 from an

external packet data network, its header fields are checked 314. When doing this, the PDG compares the header fields of the packets received from the external IP network PDN with the packet classifiers of the gates, based on which the PDG knows if the packets can be forwarded to the terminal, and, if so, which tunnel is to be applied to each IP packet. If a gate is found, whose packet classifiers the packet corresponds to, i.e. the header fields of the packet correspond to the set of packet classification parameters determined by the PDF at the PDG (PEP function), the PEP determines the identifier of the tunnel associated with the gate and directs 315 the packet to be transferred in accordance with the tunnel and the underlying WLAN network resources defined therein. If the packet identifiers do not conform to the filter conditions bound to the tunnel, the packet cannot be transferred by means of the tunnel. It is to be noted that the messages illustrated in Figure 3 are only one example of arranging the data transmission and the ongoing 3GPP-WLAN development work may lead to another kind of network structure/signalling arrangement.

**[0036]** The features illustrated in association with Figure 3 can also be utilized such that the tunnel arranged for signalling connectivity to the P-CSCF is also utilized for user data transmission between the MS and the PDG, whereby no tunnel establishment messages are required but instead messages of other type may be used between the MS and the PDG. In another embodiment, a first tunnel between the mobile station MS and a first network element (PDG) of the mobile network is established for end-to-end service parameter signalling (via the P-CSCF), and a second tunnel between the mobile station MS and a second network element of the mobile network (another PDG) is established for user data transmission after the reception of the (resource authorization) identifier.

**[0037]** The applicability of the functions illustrated above are not limited to any specific tunnelling technique. In one embodiment, tunnels are IPsec tunnels and identified by at least one IPsec tunnel specific identifier which may be used when binding authorization (and the classification parameters thereof) to the tunnel and when arranging underlying data transmission resources.

**[0038]** In this embodiment, the IPsec tunnel may be established between the MS and the PDG by utilizing the IKE (Internet Key Exchange)

protocol. First the MS and the PDG perform a key exchange by Diffie-Hellman procedure and generate an IKE security association. In one embodiment, the IKE security association is authenticated by using an EAP (Extensible Authentication Protocol) SIM or EAP AKA (Authentication and Key Agreement) procedure. After this, separate security associations are negotiated for user traffic. These associations are referred to as CHILD SAs. In the present embodiment, the SIP signalling could have a specific CHILD AS, and no policy control would be needed for the SIP signalling. Thus, the token could be transferred to the mobile station (step 302 in Figure 3) by a payload packet protected by the IPsec using the CHILD AS. In one embodiment, the token transferred from the mobile station MS to the PDG is included in a field of a CREATE CHILD AS negotiation message used for negotiating security association between the MS and the PDG. One or more new data fields can be reserved in these messages for transferring the token. In another embodiment, INFORMAL negotiation of the IPsec is used to deliver the parameters required for arranging the policy control by the PDG. These parameters can be associated with an earlier negotiated CHILD SA which could be the one already negotiated for the SIP session.

**[0039]** Thus, the token could be bound to a CHILD AS security association identified by an SPI (security parameter index) and possibly with the mobile station's and/or PDG's IP address. This SPI is also included in user-plane packets of the IPsec ESP (encapsulating security payload) or AH protocols.

**[0040]** In an embodiment, different media types/components, typically audio, video and data, are allocated with different flow identifiers. In this embodiment, the mobile terminal MS may in step 303 generate the flow identifiers for the media types. The request for establishing/modifying the tunnel may thus comprise more than one flow identifier possibly relating to the same token. With this embodiment, it is possible to separate different media types and even reserve different QoS for different media types.

**[0041]** In one embodiment, the tunnel and/or underlying connection reservations may also be modified later. The features illustrated above are applicable between the MS and PDGs in the home PLMN or in visited PLMN.

**[0042]** In an alternative embodiment differing from Figure 3, the

authorization token is sent using an already established tunnel, i.e. the end-to-end QoS adaptation based on the authorization of the PDF is separate from the tunnel establishment procedure and the data transmission resources in WLAN network AN and/or the PLMN may be adapted according to the authorization.

**[0043]** It is to be noted that the authorization identifier from the PDF may be some other identifier than the authorization token or that the authorization token may differ in contents from that for GPRS services. Further, for non-session based applications some binding information may be used.

**[0044]** The invention can be implemented in a mobile station and in network elements (in an embodiment, in the mobile station MS and in the PDG) by respective computer program codes executed in a processor of the respective device. Computer program codes can be received via a network and/or be stored in memory means, for instance on a disk, a CD-ROM disk or other external memory means, from which they can be loaded into the memory of the processing device. Hardware solutions or a combination of software and hardware solutions may also be used. A chip unit or some other kind of module for controlling the network element (or the mobile station MS) may in one embodiment cause the device to perform the inventive functions in the network element (or the mobile station MS).

**[0045]** It is obvious to a person skilled in the art that as technology advances, the basic idea of the invention can be implemented in a variety of ways. The invention and its embodiments are thus not limited to the above examples, but may vary within the claims. Different features may thus be omitted, modified or replaced by equivalents.